*XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2007**, Beograd, 11. i 12. decembar 2007.*

MULTIMEDIA DATA HIDING: TECHNIQUES AND MODELING

Andreja Samčović[1], Jan Turan[2]
[1]Faculty of Transport and Traffic Engineering, Belgrade
[2]Faculty of Electrical Engineering and Informatics, Košice, Slovakia

Abstract: *The objective of this paper is to evaluate and assess the potential of multimedia data hiding. Every few years, computer security has to reinvent itself. New technologies and new applications bring new threats, and force us to invent new protection mechanisms. A large number of schemes have been proposed for hiding information in multimedia objects. One of the newest hot spot in security research is multimedia data hiding. A model of data hiding in the presence of just noticeable distortion is taken into accoun in this paper.*

Keywords: *Data hiding, Steganography, Watermarking, Multimedia, Security*

1. Introduction

The last few years have seen rapidly growing interest in ways to hide information in other information. A number of factors contributed to this. Fears that copyright would be eroded by the ease with each digital media could be copied, led people to study ways of embedding hidden copyright marks and serial numbers in audio and video; concern that privacy would be eroded led to work on electronic cash, anonymous remailers, digital elections and techniques for making mobile computer users harder for third parties to trace; and there remain the traditional „military" concerns about hiding one's own traffic while making it hard for the opponent to do likewise.

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital audio, video, images and multimedia documents reach and ever expanding costumers, and their domination in entertainment, arts, education is just a mater of time. The rapid evolution of digital technology makes the development of reliable and robust schemes for protecting digital still images, audio and video from piracy a mater of urgency. However, it also increases the potential for unauthorized distribution of such information, and significantly increases the problems associated with enforcing copyright protection. Piracy attacks include illegal access to transmitted data in networks, data content modification and production and retransmission of illegitimate copies. The impacts of such attacks might be very large, both in financial and security terms.

Data transmitted through network communication lines may be protected from unauthorized receivers by applying techniques based on criptography. Only persons, who possess the appropriate private key, can decrypt the received data using a public algorithm implemented either in hardware or in software.

In this paper, the basic concept of multimedia data hiding is discussed. The steganography techniques, as well as digital watermarking, is referred. We will invoke also a model of multimedia data hiding, taking into account just noticeable distortion. Some final remarks conclude the paper.

2. Basic concept of data hiding

All forms of multimedia data (images, audio, video, text and multimedia documents) can be used for hiding. There are currently two areas of research which are generally referred to as „information hiding" [1]:

- *Steganography* – the main purpose is to hide or cover the occurence of communication with other data, in such a way that the third parties (unauthorized persons) cannot detect or even notice the presence of the communication. Steganographic communications are usually point-to-point. Compared with cryptography techniques attempting to conceal the content of message, steganography conceals the existence of the secret message
- *Digital watermarking* – the objective is to embed a signature within a digital cover signal to signify origin or ownership. Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks. Watermarks do not always need to be hidden (some systems use visible digital watermarks), and watermarking techniques are usually one-to-many.

The most important properties of data hiding schemes are [2]:

- *Robustness* – presence of the embedded information can be reliably detected after an image has been modified, but not destroyed beyond recognition, and means resistance to „blind", non-targeted modification, or common image operations.
- *Undetectability* – typically required for secure covert communication. The embedded information is undetectable if the data with the embedded message are consistent with a model of the source from which data are drawn, e.g. mathematical analysis may reveal statistical discrepeancies that expose the fact that hidden communication is happening.
- *Invisibility (perceptual transparency)* – an average human subject must be unable to distinguish among data that do contain hidden information and those that do not, and this property is associated with Signal-to-Noise Ratio (SNR).
- *Security* – the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the knowledge of at least one carrier with hidden message. The system is already insecure if an attacker is able to prove the existence of secret message.
- *Capacity* – maximum amount of hidden data that can be hidden and successfully extracted.

The above requirements are mutually competitive and cannot be clearly optimised at the same time, so a reasonable compromise is always a necessity. This observation is schematically depicted in Fig. 1 [1].

The information to be hidden (watermark, fingerprint, or in the general case of steganography, a secret message) is embedded in a cover-object (a cover compact disc CD, a cover video, a cover text etc.) giving a stego-object, which is in the context of copyright marking may be called a marked object (CD, video, etc.) [3]. The cover-object (cover data, carrier) is a randomly chosen harmless data, which can be transmitted without raising suspicion. Embedding algorithm is used to hide secret data inside cover-object, usually protected by stego-key (secret key) and returns stego-object, which is transmitted over insecure channel to recipient. The key is a secret variable that is in general known to the object's owner. Extraction algorithm (detector function) as opposed to embedding algorithm is used for reconstruction of hidden secret data out of stego-object.

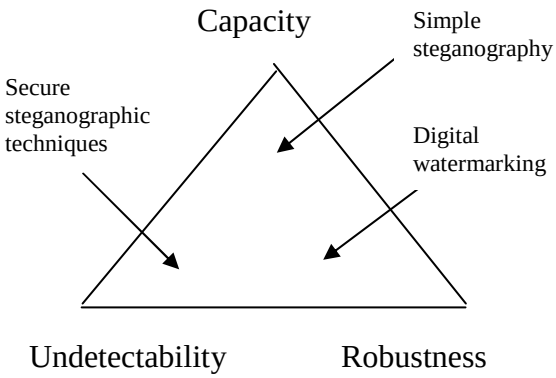

Fig. 1. *Requirements for multimedia data hiding techniques*

Recovery of the embedded mark may or may not require a key; if it does the key may be equal to, or derived from the key used in the embedding process. This scenario for hiding messages is shown in Fig. 2 [2].

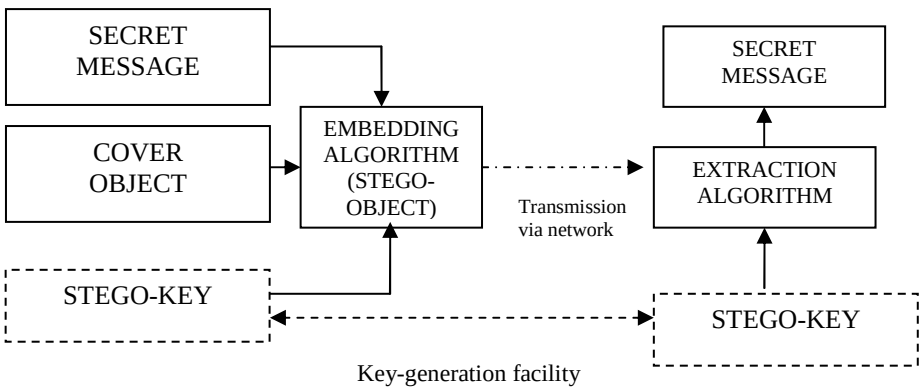

Fig. 2. *Scenario for messages hiding*

3. Steganographic techniques

The word „steganography“ is derived from two Greek words: „steganos“ which means „covered“ and „graphos“ which means „writing“, i.e. covered writing. It is the art of concealed communication; the very existence of a message is secret. Some examples of old steganography techniques include: writing on shaved heads, invisible ink and microscopic images.

There are basically three types of steganographic protocols:

- *Pure steganography* – represents systems, which don't require the prior exchange of some secret information (like a stego-key). Both sender and receiver must have access to the embedding and extraction algorithm, but the algorithms should not be public. Security of the system depends entirely on its privacy.
- *Secret key steganography* – sender embeds the secret message using a secret key (stego-key). If this key is known to the receipent, he can reverse the process and extract the secret message, but anyone who does not know the secret key should not be able to obtain evidence of the encoded information. Some algorithms additionally require the knowledge of the original cover in the decoding phase.
- *Public key steganography* – these systems require the use of two keys, one private and one public key. Whereas the public key is used in the embedding process, the secret key is used to reconstruct the secret message. One way to build such a system is the use of public key cryptosystem.

There are several approaches in classyfing steganographic techniques. They can be categorised in six categories:

- *Substitution systems* – substitute redundant parts of a cover with a secret message. Several methods can be mentioned, such as LSB (Least Significant Bit) substitution, image downgrading, palette-based techniques or quantization, and dithering of data techniques.
- *Transform domain techniques* – embed secret information in a transform domain of a signal (e.g. in the frequency domain) and are most robust than substitution systems. The most popular methods are Discrete Cosine Transform (DCT), phase coding or echo hiding techniques for digital sound.
- *Spread spectrum techniques* – adopt ideas from spread spectrum communication. Even if small parts of the signal can be removed in several frequency bands, enough information should be present in the other bands to recover the signal. Thus, spread spectrum makes it difficult to detect and remove the signal. Two special variants are generally used: directe sequence and frequency-hoping schemes.
- *Statistical methods* – encode information by changing several statistical properties of a cover and use hypothesis testing in extraction process. The cover is split into blocks, and each block is used to hide one message bit. This method is difficult to be applied in many cases, since a good test must be found which allows distinction between modified and unmodified cover blocks.
- *Distortion techniques* – store information by signal distortion and measure the deviation from the original cover in the decoding step (e.g. encoding information in formatted text). It is not useful in many applications, since the decoder must have access to the original cover.

- *Cover generation methods* – encode information in a way that a cover for secret communication is created (e.g. mimic functions). One example is automated generation of text. Message bits are transformed into sentences by selecting words out of the dictionary.

One example of a simple steganographic mechanism is shown in Fig. 3 [2].

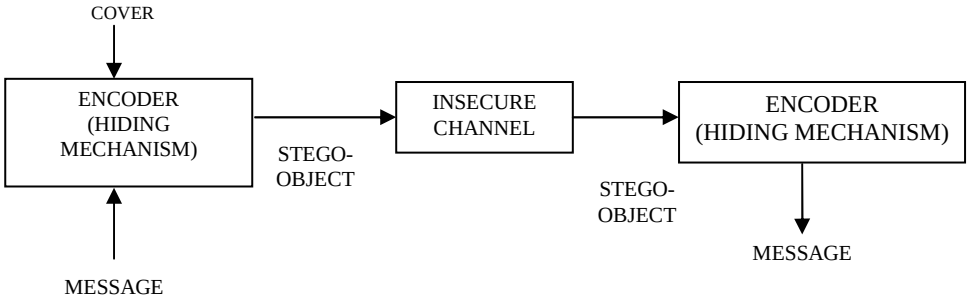

Fig. 3. *Simple steganographic mechanism*

4. Watermarking techniques

Watermarks are digital signals that are superimposed on other digital signal causing alterations to the original data. A particular watermark belongs exclusively to one owner who is the only person that can proceed to a trustworthy detection of its personal watermark, and thus prove the ownership of the host signal. The owner is also the only person that can remove the watermark from the digital data.

Digital watermarking is a method for embedding hidden data that contain copyright related information into a digital object. This provides an ownership identification of the object, and possibly other information that conveys conditions of use. Therefore, watermarking enables identification and tracing of different copies of distributed data. Watermark embedding can generally take place either in the spatial or in the transform domain. In the spatial domain, the watermark signal is directly embedded into the value of each pixel in an image, while in the frequency domain the watermark signal is embedded into the coefficients of the transformed image. Empirically, the transform domain approaches are more robust against noise or attack.

Digital watermarking has many applications. The requirements on digital watermarking are number of desirable characteristics that a watermark should exhibit. Since different applications have different requirements, there is no unique set of requirements that all watermarking techniques must satisfy.

Beside mentioned features, watermarks should possess the following [4]:

- *Trustworthy detection* – watermarks should constitute a sufficient and trustworthy proof of ownership on a particular product. Detection false alarms (false positives) should appear extremely rarely (hopefully never). Watermark signals should be characterised by great complexity. This is necessary in order to be able to produce an extensive set of sufficiently well distinguishable watermarks. An enormous set of watermarks prevents the recovery of particular watermark by trial and error procedures.

- *Associated key* – watermarks should be associated with an identification number, socalled watermark key. The key is used to cast, detect and remove a watermark. Subsequently, the key should be private and characterised exclusively the legal owner. Any digital signal, extracted from a digital signal, is assumed to be a valid watermark if and only if it is associated to a key via a well established algorithm.
- *Automated detection/search* – watermarks should combine easily with a search procedure that scans any publicly accessible domain in a network environment for illegal deposition of an owner's product.
- *Multiple watermarking* – one should be able to embed a sufficient number of different watermarks in the same signal. This feature seems necessary because we cannot prevent someone from watermarking an already watermarked signal. It is also convenient in cases where the copyright property is transferred from one owner to another (a fingerprinting-like process). It is mentioned that the legal signal owner is only one that can dispose a copy containing only his/her watermark.

The basic principle of watermarking mechanism is illustrated in Fig. 4 [2].

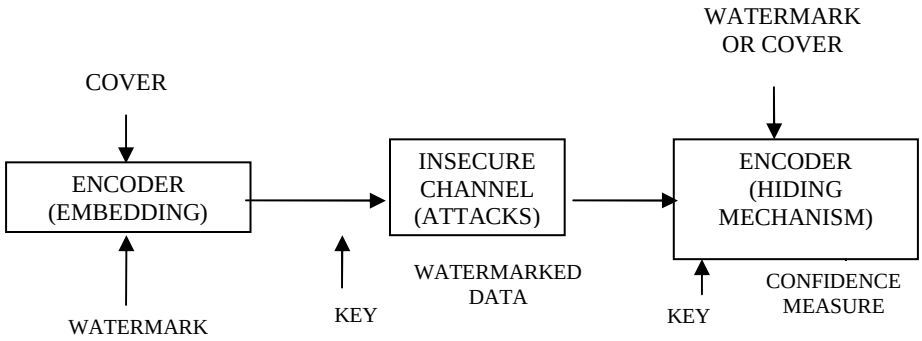

Fig. 4. *Basic principle of watermarking mechanism*

Watermarking is closely related to steganography, but there are differences between them: in watermarking the message is related to the cover, and steganography typically relates to cover point-to-point communication between two parties. Therefore, steganography requires only limited robustness. Watermarking is often used whenever the cover is available to parties who know the existence of the hidden data and may have an interest in removing it. Taking it into account, watermarking has the additional notion of resilience against attempts to remove the hidden data. Watermarks are inseparable from the cover in which they are embedded. Unlike cryptography, watermarks can protect content even after they are decoded.

Interest in digital watermarks has grown out of an increasing interest in intellectual property and copyright protection [5]. Digital watermarks may be perceptible (visible) or imperceptible (invisible) to human vision. Visible watermarks, by nature, are more intrusive to the media and act to deter theft of the media, such as a warning sign announces an alarm system even if one does not exist. Examples of such watermarks can

be seen easily on most network television stations by the station's logo in the corner of the viewable screen. These watermarks are typically confined to an area of the image, which is less intrusive to the overall image. Attackers have a visible target and can remove the watermark by cropping the image.

Invisible watermarks have an advantage over visible watermarks, in that their location may be unknown. A common practice is to distribute the watermark (or watermarks) across the entire image. This provides some protection against cropping attacks. However, the less perceptible a watermark is, it may be more vulnerable to manipulation. If information is added to some media such that the added information cannot be detected, then there exists some amount of additional information that may be added or removed within the same threshold, which will owerwrite or disable the embedded information. If the attacker intents to disable the watermark, this can be easily done. One way around this is to produce a more perceptible watermark thus impacting some part of the visible portion of the image [6].

5. Modeling

Communicating the hidden signal information is likened to transmission of the signal through an associated communications channel as is shown in Fig. 5 [7]. Embedding the signal is equivalent to the channel coding and extraction of the hidden information serves the same purposes as a communications receiver. For most data hiding applications, the only potential source of manipulation after embedding is perceptual coding. In this case, the process of lossy compression characterizes the associated communications channel for the hidden data.

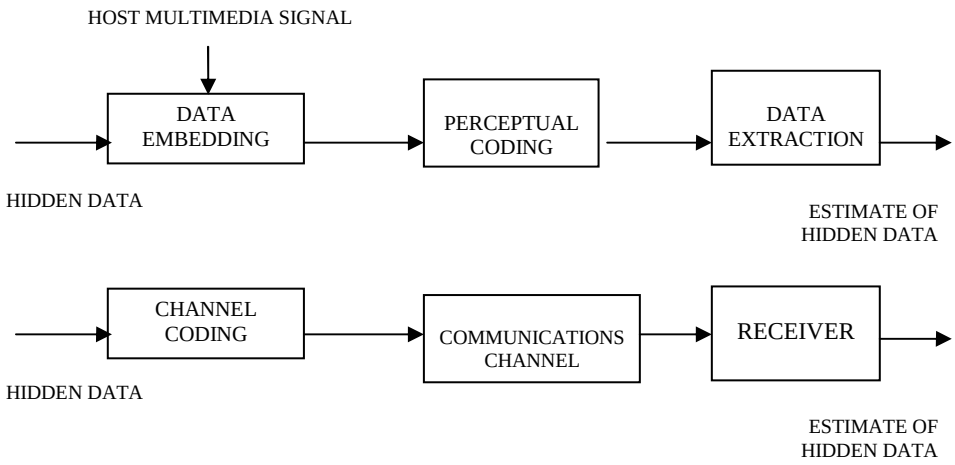

Fig. 5. *Communications analogy for data hiding*

The particular measure we are concerned with is that of transmission capacity. Employing the just noticeable distortion JND, we can treat the problem as an information theoretic one.

Communication channel is considered to be confused of smaller sub-channels denoted as C_i, for i = 1,2,...,M, where M is the number of sub-channels. Consider the discrete signal f (i) transformed with T to produce the set of coefficients F (u). Each F(u) will have an associated JND, denoted by J* (u), such that we can form F' (u) as follows

$$F'(u) = F(u) + \beta(u) \cdot J^*(u) \tag{1}$$

where β (u) is any signal with coefficient between the values -1 and 1. The inverse transform T^{-1} of F' (u) produces the signal f' (i) which is guaranteed to be perceptually identical to f (i). The idea is to make the JND values as large as possible to exploit the masking characteristic of a broad class of signals. We assume the individual perceptual models used for data hiding and compression are conservative. Specifically, if the data hiding algorithm is restricted to making changes to the coefficient F (u) below or equal in magnitude to α (u), then the compression algorithm must have an effective JND for quantization of J (u) = J* (u) – α (u) to be both efficient and yet cause no visual distortions.

Assume that the coeficient F (u) is granted into disjoint sets G_i such that if F (u) $\in$ G_i, then

$$\frac{\alpha(u)}{J(u)} = \varepsilon_i \tag{2}$$

for some positive value ε_i which we call the relative perceptual efficiency. The values of ε_i do not necessarily have to be distinct for each i. The number of elements is sufficiently large that a perceptual length channel code may be used to transmit watermark information. Let W (u) represents the signal change in F (u) to embed hidden data. After compression, assuming no interference from the host signal, the received signal is

$$\hat{W}(u) = W(u) + Q(u) \tag{3}$$

where Q (u) is additive uniformly distributed noise and is assumed to be independent of W (u). In what follows, we will drop the argument u.

Consider $|W| \le \alpha$. The probability density function p (pdf) of Q is given by

$$p(Q) = \begin{cases} \dfrac{1}{2J}, \; for \; |Q| \le J \\ 0, otherwise \end{cases} \tag{4}$$

Tacking into account the independence of W and Q, it will be

$$p_{\hat{W}} = p_W \cdot p_Q \tag{5}$$

where we use the notation that p_X is the pdf of random variable $X \in (\hat{W}, W, Q)$.

Due to using the similar transforms for data hiding and compression, the general trend is to embed the watermark in the same domain as for performing perceptual coding [8].

Data hiding of the information signal *W* into the digital multimedia signal *f* occurs in the transform domain T. Specifically, the data *W* is hidden in the discrete coefficients *F*(*u*) produced by applying the invertible T on *f*. The new coefficient from the embedding process $\hat{F}$ (*u*) are transformed by using the inverse of T to produce the output of the data hiding process denoted as $\hat{f}$. For each coefficient *F* (*u*), the signal change due to watermark embedding to produce $\hat{F}$ (*u*) does not exceed α (*u*) which is below the JND threshold *J** (*u*) for that coefficient.

Perceptual coding of a signal $\hat{f}$ occurs in the same domain as data hiding, after signal embedding. The embedded signal $\hat{f}$ is transformed with T to produce coefficients which are then quantized to reduce the signal storage requirements. If there was no data hiding, α (*u*) = 0, for all *u*. The lossy compression would be equivalent to standard JND perceptual coding by using *J** (*u*). The only source of error on the extracted information is due to lossy compression. The host signal does not provide any interference to the hidden data.

5. Conclusion

This paper seeks to provide that invisible communication is possible in the computer age, and gave an overview of different steganographic and watermarking methods proposed in the open literature during the last few years. New ways to represent efficiently the characteristics of the watermarking algorithms are under development. A development in the area of data hiding will continue and research in building more robust methods that can survive manipulation and attacks continues to grow. The used complementary domains for the hiding and compression process may allow to hide information without sacrificing compression efficiency.

Acknowledgement

The author would like to thank to the Ministry of the Science of the Republic of Serbia and the National Program of the Republic of Slovakia for the support throughout this work.

References

[1] S.Katzenbeisser, F.Petitcolas: *"Information hiding technique for steganography and digital watermarking"*, London, Artech House, 2000.

[2] J.Dittmann, P.Wohlmacher, K.Nahrstedt: "Using cryptographic and watermarking algorithms", *IEEE Multimedia*, Vol.8, No. Oct-Dec, pp 54-65, 2001.

[3] N.Nikolaidis, S.Tsekeridou, A.Nikolaidis: "Applications of chaotic signal processing techniques to multimedia watermarking", *IEEE workshop on Nonlinear dynamics in electronic systems*, pp 1-7, Catalania, 18-20. May 2000.
[4] Z.Bojković, J.Turan, A.Samčović, L.Ovsenik: "Coding, streaming and watermarking – some principles in multimedia signal processing", *Acta Electrotechnica et Informatica*, Vol.4, No.3, Kosice, Slovak Republic, pp 13-20, 2004.
[5] B.Macq, J.Dittmann, E.Delp: "Benchmarking of image watermarking algorithms for digital rights management", *Proceedings of the IEEE*, Vol.92, No.6, pp 971-984, June 2004.
[6] Z.Bojković, A.Samčović: "Watermarking technologies for copyright protection", *XXXVII International scientific conference on Information, communication and energy systems and technologies ICEST 2002*, Vol.1, pp 131-134, Niš, Yugoslavia, 1-4. October 2002.
[7] Z.Bojković, A.Rogan: "Multimedia data hiding process", *WSEAS Transactions on Communications*, Vol.5, No.9, pp 1794-1799, September 2006.
[8] V.Dormstaedter et al: "Low cost spatial watermarking", *Computers and Graphics*, Vol.22, No.4, pp 417-424, 1998.

Sadržaj: *Cilj ovog rada je da razmotri potencijalne mogućnosti skrivanja multimedijalnih podataka. Svakih nekoliko godina neophodno je unaprediti računarsku bezbednost. Nove tehnologije i nove primene zahtevaju nove mehanizme zaštite. U poslednje vreme je predložen veliki broj algoritama za skrivanje informacija kod multimedijalnih objekata. Jedna od aktuelnih tema kod istraživanja računarske sigurnosti jeste skrivanje multimedijalnih podataka. U ovom radu je uzeto u obzir modeliranje skrivanja podataka u prisustvu jedva primetnog oštećenja informacija.*

Ključne reči: *Skrivanje podataka, steganografija, vodeni žig, multimedija, bezbednost*

SKRIVANJE MULTIMEDIJALNIH PODATAKA: TEHNIKE I MODELIRANJE

Andreja Samčović, Jan Turan